

REMARKS

This Amendment is filed in response to the Office Action mailed on April 23, 2003. All objections and rejections are respectfully traversed.

Claims 1-67 are in the case.

Independent claims were amended to better claim the invention.

At paragraph 1 of the Office Action, formal drawings were required. Accordingly, Formal Drawings are filed herewith.

At paragraphs 2-7 of the Office Action claims 2, 7-9, 13-15, 22-24, 28-30, 37-42, 49-54, 61-66 were rejected under 35 U.S.C. 112 first paragraph on the grounds that the specification does not enable a teaching of proof of "non-membership" of a group which is specifically excluded from access to the resource.

Applicant respectfully urges that non-membership of a group which is specifically excluded from access to the resource is defined in the Specification at page 6 lines 17-21 as:

The exemplary embodiment is directed to the client-server situation wherein the client is not individually authorized for access to a resource but may gain access by means of a group membership certificate (necessary for access to a particular resource) or a group non-membership

certificate (when a group is specifically excluded from access to a resource).

Applicant respectfully urges that the Specification, at page 6 lines 17-21, is clear that when a group is specifically excluded from access to a resource, then in order for a client to gain access to the resource it must present a “group non-membership certificate” in order to gain access to the resource.

The nature of the “group non-membership certificate” is set out in the Specification at page 7 lines 4-7 as a “list of members” as:

A group membership or group non-membership certificate usually indicates membership status for a specified name, e.g., client “Alice” is a member of group G1, although the certificate may also indicate membership status for a specified public key or other identity.

How a resource server makes use of a “group non-membership” certificate to prohibit access to a resource based on client membership in one or more groups is fully set out on page 10 lines 4-28 as:

Group Non-membership Certificates

A resource server may also prohibit access to a resource based on client membership in one or more groups. In this case, the client will gather and present group non-membership certificates stating that the client is not a member of the designated groups. For example, group G1 members may be permitted access to a resource, unless they are also group G2 members. Alice will have to prove both membership in group G1 and NON-membership in group G2. To prove non-membership in group G2, Alice will present a group G2 non-membership certificate to Bob. Alice

requests a non-membership certificate from the G2 group server and presents the certificate, along with a group G1 membership certificate to Bob.

The work required to gather the credentials necessary to prove group non-membership is more intensive than that required for group membership. For each prohibited root group, the client will be required to prove non-membership in each and every group extending from the root. For example, Bob may deny resource access to all members of group G2. Therefore, Alice will request a group non-membership certificate from the G2 server. The root group G2 might have as members the child groups, or subgroups, G7 and G8. The G2 group server will ask Alice: "Can you prove non-membership in groups G7 and G8?"

Alice then requests a group non-membership certificate from both the G7 and G8 servers. If group G7 also lists the groups G9 and G10, Alice requests a group non-membership certificate from both the G9 and G10 servers. Alice presents the G9 and G10 group non-membership certificates to the G7 server which then issues a group non-membership certificate. Alice next presents the G7 and G8 group non-membership certificates to the G2 server and receives a G2 group non-membership certificate. Now, armed with a group non-membership certificate from group G2, Alice can go to Bob and prove non-membership in root group G2.

The logic used to implement exclusion of a "suspect group" from access to the resource is set out on page 17 line 20 - page 18 line 10 as:

For example, resource server Bob 110 may refuse access to the resource 112 if client Alice 104 is a member of some suspect group. By having the group server responsible for the membership list for the suspect group issue a non-membership certificate, resource server Bob 110 can implement Boolean logic to prevent any client unable to present a non-membership certificate from accessing the resource. For example, if all members of group G3 are denied access to the resource and members of groups G1 and G2 are permitted access to the source, then the Boolean expression:

(G1 AND G2) AND NOT (G3)

will be FALSE in the event that resource server Bob 110 does not receive a valid non-membership certificate indicating that client Alice 104 is not a member of group G3. The FALSE result in the Boolean expression will

prevent client Alice 104 from gaining access to the requested resource on resource server Bob 110.

Accordingly, Applicant respectfully urges that the Specification is fully enabling, as required under 35 U.S.C. § 112 first paragraph, on the issue of how one would determine and produce the non-member groups, certificates, etc., and how to use them in preventing a “suspect group” from accessing a resource.

At paragraphs 8-11 of the Office Action, claims 1-54 were rejected under 35 U.S.C. § 102(b) as being anticipated by Gassser et al. U. S. Patent No. 5,220,604 issued on June 15, 1993 (hereinafter Gasser).

Applicants invention, as set out in representative claim 1, comprises in part:

1. A method of obtaining proof of group membership in a computer system, comprising the steps of:

- A. presenting by a requester to *an on-line server* associated with a group a request for a certificate certifying that a particular entity is a member of the group;
- B. determining by the server whether the entity is a member of the group; and
- C. *issuing by the server at runtime a newly-issued group membership certificate to the requester if the server determines that the entity is a member of the group.*

Gasser discloses a “global naming service” (hereinafter GNS) which maintains copies of group membership certificates signed by an authority located else-

where in a “clean” environment. When a client seeks access to a resource, the resource makes an inquiry to the GNS, the GNS searches certificates of authority for that resource, and if the client is found listed on a certificate, then access to the resource is granted.

Applicant respectfully urges that Gasser has no disclosure of Applicant’s novel use of an *on-line server* which performs the step of *issuing by the server at runtime a newly-issued group membership certificate to the requester if the server determines that the entity is a member of the group*. That is, Gasser has no disclosure of an *on-line server . . . issuing by the server at runtime a newly-issued group membership certificate*.

In contrast, Gasser simply discloses a GNS holding old membership certificates which have been signed elsewhere at an earlier time, and upon request searching the certificate for an entity in order to determine if the entity is a member of a group, and then sending a copy of the old certificate to the requestor.

Accordingly, Applicant respectfully urges that Gasser is legally precluded from anticipating the presently claimed invention under 35 U.S.C. § 102(b) because of the absence from Gasser of Applicant’s claimed novel *on-line server* performing the step of *issuing by the server at runtime a newly-issued group membership certificate to the requester if the server determines that the entity is a member of the group*.

At paragraphs 12-14 of the Office Action, claims 55-66 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Gasser as applied to rejected claims 1-54 above.

Applicant respectfully urges that claims 1-54 are in condition for allowance because of the absence from Gasser of Applicant's claimed novel *on-line server* performing the step of *issuing by the server at runtime a newly-issued group membership certificate to the requester if the server determines that the entity is a member of the group*. Accordingly, Applicant respectfully urges that Applicant's use of a carrier wave to implement a novel process is also novel, and that claims 55-66 are in condition for allowance.

Further, Applicant respectfully urges that Gasser teaches away from the present invention, as Gasser teaches only the sending of copies of old certificates. A person of ordinary skill in the art at the time that the invention was made would be led, by following Gasser, to simply design a better way to send old certificates which were signed elsewhere. That is, Applicant's new novel innovation of having an on-line server issue a *new* group membership certificate would never occur to a person of ordinary skill in the art who followed Gasser's teaching of sending an old certificate of membership.

Finally, Applicant respectfully urges that Gasser and claims 1-54, taken either singly or in combination are legally precluded from rendering claims 55-66 obvious un-

der 35 U.S.C. 103(a) because of the absence from Gasser of Applicant's claimed novel *on-line server* performing the step of *issuing by the server at runtime a newly-issued group membership certificate to the requester if the server determines that the entity is a member of the group*.


All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims, and therefore in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,


A. Sidney Johnston
Reg. No. 29,548
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500